

IN THE CLAIMS

This listing of the claim will replace all prior versions and listings of claim in the present application.

Listing of Claims

1. (currently amended) A security system design supporting method for supporting ~~the~~ designing of security requirements ~~and/or~~ security specifications based on an international security evaluation criteria ~~in the stage of~~ during planning/designing of an information-related product ~~and/or~~ an information system, said method comprising the steps of:

providing a template case database for storing internationally registered protection profiles (PP) or PP/STs (security targets), that have been generated ~~in the past~~ and not internationally registered, in a class-tree structure based on a relation ~~the inheritance between the types of the product~~ products or ~~the systems~~ systems as a target of evaluation (TOE) of said PP/STs;

specifying the PP/STs related to the TOE by designating ~~constituting~~ elements included in the products or systems, type and evaluation assurance level of the TOE and retrieving a relevant class-tree structure from said database; and

automatically generating a PP/ST draft of the TOE by integrally editing the contents of ~~the~~ a definition of ~~said~~ the specified PP/STs.

2. (currently amended) A security system design supporting method comprising the steps of:

providing a partial case database for storing a security environment including assumptions, threats and organizational policies corresponding to the constituting elements of a the product and/or a system accumulated by the PP/ST-applied cases, security objectives corresponding to the security environment, CC requirements corresponding to the security objectives, and the information on of a summary specification corresponding to the CC requirements;

automatically mapping from said database to ~~the~~ corresponding information by designating the ~~constituting elements~~ included in the product or system, the security environment, the security objectives and the security requirements of the TOE; and

automatically generating a portion of contents of definition of the PP/ST associated with the TOE based on the corresponding information thus mapped.

3. (currently amended) A security system design supporting method comprising ~~in combination~~ the steps of:

automatically generating a PP/ST draft by ~~the~~ a first security system design supporting method ~~according to Claim 1, which comprises the steps of;~~ and

providing a template case database for storing internationally registered protection profiles (PP) or PP/STs (security targets), that have been generated in the past and not internationally registered, in a class-tree structure based on a relation between types of products or systems as a target of evaluation (TOE) of said PP/STs.

specifying the PP/STs related to the TOE by designating elements included in the products or systems, type and evaluation assurance level of the TOE and retrieving a relevant tree from said database, and

automatically generating a PP/ST draft of the TOE by integrally editing contents of a definition of said specified PP/STs;

partially adding and/or correcting the PP/ST by the a second security system design supporting method, according to Claim 2, which comprises the steps of:

providing a partial case database for storing a security environment including assumptions, threats and organizational policies corresponding to elements of the products or systems accumulated by the PP/ST-applied cases, security objectives corresponding to the security environment, CC requirements corresponding to the security objectives, and information of a summary specification corresponding to the CC requirements,

automatically mapping from said database to corresponding information by designating the elements included in the products or systems, the security environment, the security objectives and the security requirements of the TOE, and

automatically generating a portion of contents of a definition of the PP/ST associated with the TOE based on the corresponding information thus mapped.

4. (currently amended) A security system design supporting method according to Claim 1, further comprising the steps of:

indicating the PP/STs stored in the template case database as icons by which the constituting elements, type and the evaluation assurance level can be identified;

specifying the PP/STs related to the TOE from the ~~inheritance-related class-~~
tree based on the reference PP/ST cases of the ~~inheritance-~~relations between the
PP/STs expressed in a tree; and

producing a structure diagram of the TOE using the icons of said specified
PP/STs as constituting elements.

5. (currently amended) A security system design supporting method
according to Claim 2, further comprising the steps of:

storing data concerning ~~the~~ probability of occurrence of each threat and the
loss amount affected by the threat and cost of protection ~~cost~~ of each security
objective collectively in the partial case database;

producing a formula of a combinatorial optimization problem by designating
~~the~~ constraints of a risk acceptance, a cost limit value, a ratio of residual risk to
protection cost and ~~the~~ objective functions for cost minimization or protection risk
maximization with respect to ~~the~~ a relation between ~~the~~ risk of each threat, ~~(the~~
probability of occurrence multiplied by ~~the~~ affected loss amount) and the cost of
protection ~~cost~~ of the corresponding security objectives; and

determining cost-effective optimal security objectives by solving said
combinatorial optimization problem.

6. (currently amended) A security system design supporting method
according to Claim 2, further comprising the step of:

verifying whether ~~the~~ requirements of ~~the~~ automatically generated contents of definition match ~~the~~ dependency and/or hierarchy relation between ~~the~~ functional requirements and ~~the~~ assurance requirements of the reference specifications based on the dependency and/or hierarchy relation of the reference specifications.

7. (currently amended) A security system design supporting method according to Claim 1, further comprising the steps of:

automatically generating a rationale matrix indicating in a matrix table each correspondence between ~~the~~ security environments, ~~the~~ security objectives, ~~the~~ security requirements and ~~the~~ summary specification as a part of ~~the~~ contents of the PP/ST definition from ~~the~~ a security environment, the security objectives, the security requirements and the summary specification or the correspondence between them; and

verifying ~~the~~ presence or absence of ~~the~~ definition information lacking the correspondence using ~~said a~~ rationale matrix generated.

8. (currently amended) A security system design supporting method according to Claim 2, further comprising the steps of:

automatically generating a rationale matrix indicating in a matrix table each correspondence between ~~the~~ security environments, ~~the~~ security objectives, ~~the~~ security requirements and ~~the~~ summary specification as a part of ~~the~~ contents of the PP/ST definition from the security environment, the security objectives, the security

requirements and the summary specification or the correspondence between them;
and

verifying the presence or absence of ~~the~~ definition information lacking the
correspondence using said rationale matrix generated.

9. (currently amended) A security system design supporting method
according to Claim 3, further comprising the steps of:

automatically generating a rationale matrix indicating in a matrix table each
having a correspondence between ~~the~~ security environments, ~~the~~ security
objectives, ~~the~~ security requirements and ~~the~~ summary specification as a part of the
contents of the PP/ST definition from the security ~~environment~~ environments, the
security objectives, the security requirements and the summary specification or the
correspondence between them; and

verifying ~~the~~ presence or absence of ~~the~~ definition information lacking the
correspondence using said rationale matrix generated.

10. (currently amended) A security system design supporting method
according to Claim 1, further comprising the steps of:

storing information newly added in ~~the~~ a process of PP/ST generation and ~~the~~
a result of PP/ST generation in accordance with the ~~inheritance~~ relation and
correspondence in the template case database and the partial case database; and
improving and expanding ~~the~~ information stored in the case database.

11. (currently amended) A security system design supporting method according to Claim 2, further comprising the steps of:

storing information newly added in ~~the~~ a process of PP/ST generation and ~~the~~ a result of PP/ST generation in accordance with the ~~inheritance~~ relation and correspondence in the template case database and the partial case database; and improving and expanding the information stored in the case database.

12. (currently amended) A security system design supporting method according to Claim 3, further comprising the steps of:

storing information newly added in ~~the~~ a process of PP/ST generation and ~~the~~ a result of PP/ST generation in accordance with the ~~inheritance~~ relation and correspondence in the template case database and the partial case database; and improving and expanding the information stored in the case database.

13. (original) A security system design supporting method according to Claim 1:

wherein the generated PP/ST can be evaluated in a PP/ST evaluation check list in the form of questions based on an international security evaluation method.

14. (original) A security system design supporting method according to Claim 2:

wherein the generated PP/ST can be evaluated in a PP/ST evaluation check list in the form of questions based on an international security evaluation method.

15. (original) A security system design supporting method according to Claim 3:

wherein the generated PP/ST can be evaluated in a PP/ST evaluation check list in the form of questions based on an international security evaluation method.

Claim 16 (canceled).

17. (currently amended) A security design supporting method for supporting the design of ~~the~~ security requirements and/or security specifications based on international evaluation criteria ~~in the stage of~~ during planning and/or designing of a TOE, using a database including a template case database structured in a class tree of internationally registered PPs (protection profiles) or PP/STs (security targets) not internationally registered, based on ~~the inheritance~~ a relation between types of the ~~product and/ products or system-systems~~ as a TOE of said PP/STs, said method comprising the steps of:

specifying by designating ~~the constituting elements~~ included in the products or systems, type and ~~the~~ assurance level of the TOE and retrieving the class-tree of the PP/STs related to the TOE from said database;

automatically generating a PP/ST draft of the TOE by integrally editing the contents of definition of ~~said the~~ specified PP/STs; and

expanding said case database by storing ~~the~~ information newly added in ~~the~~ a process of PP/ST generation ~~and/or the~~ a result of PP/ST generation in accordance with the ~~inheritance~~ relation of a template case database or a partial case database.

18. (currently amended) A security system design supporting method executed using a case database for storing a security environment including assumptions, threats and organizational policies corresponding to ~~constituting~~ elements of a product ~~and/or a system~~ accumulated by PP/ST-applied cases, security objectives corresponding to ~~the~~ security environment, CC requirements corresponding to the security objectives, and information on a summary specification corresponding to the CC requirements, said method comprising the steps of:

storing data concerning ~~the~~ a probability of occurrence of each threat and ~~the~~ a loss amount affected by the threat together with protection cost data of each security objective in said case database;

expressing in a formula a combinatorial optimization problem by designating constraints including risk acceptance, ~~the~~ cost limit value, ~~the~~ ratio of a residual risk to a protection cost and objective functions for protection risk maximization or cost minimization with respect to ~~the~~ relation between the risk of each threat and the protection cost of corresponding security objectives, the risk being expressed as ~~the~~ a product of ~~the~~ a probability of occurrence and ~~the~~ affected loss amount; and

determining a cost-effective optimal security objective by solving said combinatorial optimization problem.

19. (currently amended) A computer readable recording medium for storing program code means for executing the design support of security requirements and/or security specifications based on international security evaluation criteria in the stage of planning or designing a TOE using a database including a template case database class-tree ~~structured structure~~ based on a relation the inheritance between the types of the TOE of said PP/STs for storing internationally registered PPs, (protection profiles), or PP/STs produced in the past and not internationally registered, wherein said program code means includes:

program means for retrieving said tree and specifying the PP/STs related to the TOE by designating ~~constituting elements~~ included in a product or system, type and the assurance level of said TOE;

program means for automatically generating a PP/ST draft of the TOE by integrally editing ~~the contents of the definition of the PP/STs specified~~; and

program means for expanding the case database by storing information newly added in ~~the a~~ PP/ST generation process and/or ~~the a~~ result of PP/ST generation in accordance with the ~~inheritance~~ relation of the template case database or the partial case database.

20. (currently amended) A computer readable recording medium for storing program code means for executing the supporting of design of a security system using a case database for storing a security environment including assumptions, threats and organizational policies corresponding to ~~corresponding information of~~ including constituting elements of a product and/or a system as a target of evaluation

(TOE) accumulated by the PP/ST construction cases, security objectives corresponding to ~~the~~ a security environment, security requirements corresponding to the security objectives, and an implementation scheme corresponding to the security requirements, wherein said program code means includes:

program means for storing ~~the~~ a probability of occurrence of each threat and an affected loss amount data together with cost of protection ~~cost~~ data of each security objective in said case database;

program means for expressing in a formula a combinatorial optimization problem by designating constraints including a risk acceptance, cost limit value, ~~the~~ ratio of a residual risk to ~~the~~ cost of protection ~~cost~~ and an objective function for cost minimization or maximization of ~~the~~ protection risk with respect to the relation between ~~the~~ a risk of each threat and the cost of protection ~~cost~~ of the corresponding security objectives, the risk being expressed as ~~the~~ a product of ~~the~~ probability of occurrence and ~~the~~ affected loss amount; and

program means for determining cost-effective optimal security objectives by solving said combinatorial optimization problem.

21. (currently amended) A computer readable program stored on a medium and implementing a security system design supporting method for supporting the designing of security requirements ~~and/or~~ security specifications based on an international security evaluation criteria ~~in the stage of planning/designing of~~ an information-related product ~~and/or~~ an information system, comprising the steps of:

providing a template case database for storing internationally registered protection profiles (PP) or PP/STs (security targets) generated in the past and not internationally registered, in a class-tree structure based on the inheritance relation between the types of the product/products or the system-systems as a target of evaluation (TOE) of said PP/STs;

specifying the PP/STs related to the TOE by designating constituting elements, type and evaluation assurance level of the TOE and retrieving a relevant from said database; and

automatically generating a PP/ST draft of the TOE by integrally editing the contents of the definition of said specified PP/STs.

22. (new) A security design supporting method for creating a security specification of an information system or a product, comprising the steps of:

providing a database in which security specifications relating to an information system or an information product are previously registered in a class-tree structure based on an inheritance relation between constituent elements, types of product or certification levels;

when creating a security specification of an objective information system or a product as an object to be designed, sending relevant constituent elements or relevant security specifications of a product from said database using objective constituent elements, product type and acquired certification level as a search key; and

when a plurality of specifications are searched, integrally editing the searched plurality of specifications into one specification according to a format of prescribed contents in respect to descriptions of the searched specifications to thereby automatically generate a specification draft of the objective information system or product.
